TB-0357

NETWORK PERIMETER SECURITY ENHANCEMENTS

Issue Date: December 30, 2004
Effective Date: March 6, 2005
Section/Group: Enterprise Information Security Office
Submitted by: Michael Allred
Approved by: Dave Fletcher

In December 2003, ITS Technical Bulletin #332: *Enhanced Security Requirements for System Access* was issued to close down port 23 (Telnet) on the perimeter firewall. The Security Office received a good deal of support for this and hundreds of conduits have been eliminated. We continue to work with State and local agencies to eliminate all clear text external access.

As part of our ongoing effort to enhance the security of the State of Utah's perimeter defenses, effective March 6, 2005, **incoming traffic** to the following ports will be closed at the perimeter firewall.

Ports	Usage		Ports	Usage
22	Used for Secure Shell (SSH).		5800	VNC default port for client
55	VNC Servers		5850	Unspecified
123	Network Time Protocol (NTP)		5900	VNC default port for web client
443	Used for SSL access to web site		5950	Unspecified
7100	TCP - font-service		5955	Unspecified
8009	Novell Remote Manager		5631	PCAnywhere
8081	Unspecified		5632	PCAnywhere
4900	MUTE file sharing (like Kazaa)			

Today these ports allow *any* computer in the world to access *any* computer on the State network. We are making a concerted effort to move toward a policy of "***deny that***

which is not specifically allowed. " To do this we are eliminating conduits that allow for ***any*** external access to ***any*** internal address. We will allow access from specific IP address to specific IP address.

If an agency needs specific access lists built for the ports listed above, the agency's security officer must submit a list of ***source and destination*** IP addresses that need to remain open. The request should be sent to dsecure@utah.gov and include the IP addresses to remain open, a contact name, phone number, e-mail address, and a brief reason that will be used for tracking. **This must be done prior to the March 6th deadline**. Multiple requests may be submitted in one e-mail.

After March 6, 2005, a standard firewall request form will be used to allow these ports to be open.

Alternative

ITS offers VPN service which agencies are encouraged to use. VPN creates a secure path of communication from a client machine to a VPN server for the applications that need to communicate across that path. Random users cannot simply access a VPN, as information is needed to allow a remote user access to the network, or even to begin VPN authentication. VPNs are widely considered secure.

The ITS VPN service allows authenticated users access to internal systems without additional firewall openings. Using the ITS VPN service allows the State to minimize the number of holes (ACLs) in the ITS firewall and increases the overall security of the State network.

Other Information

The Security Office also encourages State agencies to be aware of additional security risks associated with allowing external access to servers and desktops on the State network. Remote control programs like VNC, PCAnywhere, gotomypc, and terminal services, can be great productivity tools for local administrators, but they can also be used by external sources to compromise the State network. They should be used sparingly and monitored constantly.

To find out more about ITS provided VPN services, please visit the VPN product page at its.utah.gov/productsservices/datanetwork/vpnclientservices/vpnclientservices.htm or contract your Customer Relationship Manager.